Propositional Calculus I

CS 2LC3

Ryszard Janicki

Department of Computing and Software, McMaster University, Hamilton, Ontario, Canada

Propositional Calculus

- **Calculus:** method of reasoning by calculation with symbols
- **Propositional Calculus:** calculating
  - with Boolean expressions
  - containing propositional variables
- The Textbook's Propositional Calculus is called "Equational Logic **E**"
- Propositional Calculus = Axioms + Inference Rules
- Axioms: axioms for Boolean operators
- Inference Rules:
  - **Leibnitz:** $$\frac{P = Q}{E[r := P] = E[r := Q]}$$
  - **Transitivity:** $$\frac{P = Q, Q = R}{P = R}$$
  - **Substitution:** $$\frac{P}{P[r := Q]}.$$

Theorems

- A **theorem** of our propositional calculus is either
  1. an axiom,
  2. the conclusion of an inference rule whose premises are theorems, or
  3. a boolean expression that, using the inference rules, is proved equal to an axiom or a previously proved theorem.
- All theorems of our propositional calculus are valid. This fact can be established by
  - checking each axiom with a truth table and
  - arguing for each inference rule that if its premises are valid then so is its conclusion.
- All valid expressions are theorems of our calculus (although we do not prove this fact).

Equivalence Axioms

- To keep reference to the textbook easier, we will use the same numbering of formulae and theorems.

(3.1) **Axiom, Associativity of** $\equiv$: $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$: $\boxed{p \equiv q \equiv q \equiv p}$

Can be used as:

- $(p \equiv q) = (q \equiv p)$
- $p = (q \equiv q \equiv p)$
- $(p \equiv q \equiv q) = p$

Example theorem — shown differently in the textbook:

Proving $p \equiv p \equiv q \equiv q$**:**

$$
\begin{array}{ll}
 & p \equiv p \equiv q \equiv q \\
= & \langle \text{ (3.2) Symmetry of } \equiv, \text{ with } p,\ q\ :=\ p,\ q \equiv q \ \rangle \\
 & p \equiv q \equiv q \equiv p \quad \text{— This is (3.2) Symmetry of } \equiv
\end{array}
$$

Equivalence Axioms — Example Proof with Parentheses

(3.1) **Axiom, Associativity of** $\equiv$: $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$: $\boxed{p \equiv q \equiv q \equiv p}$

Can be used as:

- $(p \equiv q) = (q \equiv p)$
- $p = (q \equiv q \equiv p)$
- $(p \equiv q \equiv q) = p$

Example theorem — shown differently in the textbook:

Proving $p \equiv p \equiv q \equiv q$**:**

$$
\begin{array}{ll}
 & p \equiv (p \equiv (q \equiv q)) \\
\equiv & \langle \text{ (3.2) Symmetry of } \equiv, \text{ with } p,\ q\ :=\ p,\ (q \equiv q)\ \rangle \\
 & p \equiv ((q \equiv q) \equiv p) \quad \text{— This is (3.2) Symmetry of } \equiv
\end{array}
$$

Equivalence Axioms - Introducing *true*

(3.1) **Axiom, Associativity of** $\equiv$: $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$: $\boxed{p \equiv q \equiv q \equiv p}$

Can be used as:

- $(p \equiv q) = (q \equiv p)$
- $p = (q \equiv q \equiv p)$
- $(p \equiv q \equiv q) = p$

(3.3) **Axiom, Identity of** $\equiv$: $\boxed{true \equiv q \equiv q}$

Can be used as:

- $(true \equiv q) = q$
- $true = (q \equiv q)$

Equivalence Axioms and Theorem *truth*, ie. (3.4)

(3.1) **Axiom, Associativity of** $\equiv$: $\boxed{((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))}$

(3.2) **Axiom, Symmetry of** $\equiv$: $\boxed{p \equiv q \equiv q \equiv p}$

(3.3) **Axiom, Identity of** $\equiv$: $\boxed{true \equiv q \equiv q}$

Can be used as: $true = (q \equiv q)$

The least interesting theorem:

Proving (3.4) *true*:

$$
\begin{array}{ll}
 & true \\
= & \langle \text{ Identity of } \equiv \text{ (3.3), with } q := true \ \rangle \\
 & true \equiv true \\
= & \langle \text{ Identity of } \equiv \text{ (3.3), with } q := q \ \rangle \\
 & true \equiv q \equiv q \quad \text{— This is Identity of } \equiv \text{ (3.3)}
\end{array}
$$

Negation Axioms

(3.8) **Axiom, Definition of** *false*: $\boxed{false \equiv \neg true}$

(3.9) **Axiom, Commutativity of** $\neg$ **with** $\equiv$: $\boxed{\neg(p \equiv q) \equiv \neg p \equiv q}$

Can be used as:

- $\neg(p \equiv q) \quad = \quad (\neg p \equiv q)$
- $(\neg(p \equiv q) \equiv \neg p) \quad = \quad q$
- $(\neg(p \equiv q) \equiv q) \quad = \quad \neg p$

(3.10) **Axiom, Definition of** $\not\equiv$: $\boxed{(p \not\equiv q) \equiv \neg(p \equiv q)}$

Heuristic of Definition Elimination

- **Heuristic:** Identify applicable theorems by matching the structure of expressions or subexpressions. The operators that appear in a boolean expression and the shape of its subexpressions can focus the choice of theorems to be used in manipulating it.
- **Principle:** Structure proofs to avoid repeating the same subexpression on many lines.
- **Heuristic of Definition Elimination:** To prove a theorem concerning an operator $\circ$ that is defined in terms of another, say $\bullet$, expand the definition of $\circ$ to arrive at a formula that contains $\bullet$; exploit properties of $\bullet$ to manipulate the formula; and then (possibly) reintroduce o using its definition.
- It is called: "**Unfold-Fold strategy**"

Inequivalence Theorems: Symmetry

(3.16) **Symmetry of $\not\equiv$:** $(p \not\equiv q) \equiv (q \not\equiv p)$

Proving (3.16) Symmetry of $\not\equiv$:

$$
\begin{array}{ll}
 & p \not\equiv q \\
= & \langle \text{ (3.10) Definition of } \not\equiv \ \rangle \qquad \cdots\cdots \textbf{Unfold} \\
 & \neg(p \equiv q) \\
= & \langle \text{ (3.2) Symmetry of } \equiv \ \rangle \\
 & \neg(q \equiv p) \\
= & \langle \text{ (3.10) Definition of } \not\equiv \ \rangle \qquad \cdots\cdots \textbf{Fold} \\
 & q \not\equiv p
\end{array}
$$

Disjunction Axioms

(3.24) **Axiom, Symmetry of** $\vee$: $\boxed{p \vee q \equiv q \vee p}$

(3.25) **Axiom, Associativity of** $\vee$: $\boxed{(p \vee q) \vee r \equiv p \vee (q \vee r)}$

(3.26) **Axiom, Idempotency of** $\vee$: $\boxed{p \vee p \equiv p}$

(3.27) **Axiom, Distributivity of** $\vee$ **over** $\equiv$: $\boxed{p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r}$

(3.28) **Axiom, Excluded Middle**: $\boxed{p \vee \neg p}$

The Law of the Excluded Middle (LEM)

Aristotle:

> ...there cannot be an **intermediate** between contradictories, but of one subject we must either affirm or deny any one predicate...

Bertrand Russell in "The Problems of Philosophy":

> Three "Laws of Thought":
>
> 1. Law of identity: "Whatever is, is."
> 2. Law of noncontradiction: "Nothing can both be and not be."
> 3. Law of excluded middle: "Everything must either be or not be."
>
> These three laws are samples of self-evident logical principles...

(3.28) **Axiom, Excluded Middle**: $\boxed{p \vee \neg p}$

— this will often be used as: $p \vee \neg p \equiv true$

Disjunction Axioms and Theorems

(3.24)	**Axiom, Symmetry of** $\vee$:	$p \vee q \equiv q \vee p$
(3.25)	**Axiom, Associativity of** $\vee$:	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
(3.26)	**Axiom, Idempotency of** $\vee$:	$p \vee p \equiv p$
(3.27)	**Axiom, Distr. of** $\vee$ **over** $\equiv$:	$p \vee (q \equiv r) \equiv p \vee q \equiv p \vee r$
(3.28)	**Axiom, Excluded Middle**:	$p \vee \neg p$

Theorems:

(3.29)	**Zero of** $\vee$:	$p \vee \mathit{true} \equiv \mathit{true}$
(3.30)	**Identity of** $\vee$:	$p \vee \mathit{false} \equiv p$
(3.31)	**Distrib. of** $\vee$ **over** $\vee$:	$p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$
(3.32)	**(3.32)**	$p \vee q \equiv p \vee \neg q \equiv p$

Heuristics of Directing Calculations

(3.33) **Heuristic:** To prove $P \equiv Q$, transform the expression with the most structure (either P or Q) into the other.

Proving (3.29) $p \vee true \equiv true$**:**

$$
\begin{array}{ll}
 & p \vee true \\
\equiv & \langle \text{ Identity of } \equiv \text{ (3.3) } \rangle \\
 & p \vee (q \equiv q) \\
\equiv & \langle \text{ Distr. of } \vee \text{ over } \equiv \text{ (3.27) } \rangle \\
 & p \vee q \equiv p \vee q \\
\equiv & \langle \text{ Identity of } \equiv \text{ (3.3) } \rangle \\
 & true
\end{array}
$$

Proving (3.29) $p \vee true \equiv true$**:**

$$
\begin{array}{ll}
 & true \\
\equiv & \langle \text{ Identity of } \equiv \text{ (3.3) } \rangle \\
 & p \vee p \equiv p \vee p \\
\equiv & \langle \text{ Distr. of } \vee \text{ over } \equiv \text{ (3.27) } \rangle \\
 & p \vee (p \equiv p) \\
\equiv & \langle \text{ Identity of } \equiv \text{ (3.3) } \rangle \\
 & p \vee true
\end{array}
$$

?

(3.34) **Principle:** Structure proofs to minimize the number of rabbits pulled out of a hat — make each step seem obvious, based on the structure of the expression and the goal of the manipulation.

General Heuristic

Identify applicable theorems by matching the structure of expressions or subexpressions. The operators that appear in a boolean expression and the shape of its subexpressions can focus the choice of theorems to be used in manipulating it.

Obviously, the more theorems you know by heart and the more practice you have in pattern matching, the easier it will be to develop proofs.

The Conjunction Axiom: The "Golden Rule"

(3.35) **Axiom, Golden rule**: $\boxed{p \wedge q \quad \equiv \quad p \equiv q \quad \equiv \quad p \vee q}$

Can be used as:

- $p \wedge q \quad = \quad (p \equiv q \quad \equiv \quad p \vee q)$ — **Definition of $\wedge$**
- $(p \equiv q) \quad = \quad (p \wedge q \quad \equiv \quad p \vee q)$
- ...

Theorems:

(3.36) **Symmetry of $\wedge$**: $p \wedge q \quad \equiv \quad q \wedge p$

(3.37) **Associativity of $\wedge$**: $(p \wedge q) \wedge r \quad \equiv \quad p \wedge (q \wedge r)$

(3.38) **Idempotency of $\wedge$**: $p \wedge p \quad \equiv \quad p$

(3.39) **Identity of $\wedge$**: $p \wedge \mathit{true} \quad \equiv \quad p$

(3.40) **Zero of $\wedge$**: $p \wedge \mathit{false} \quad \equiv \quad \mathit{false}$

(3.41) **Distributivity of $\wedge$ over $\wedge$**: $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge (p \wedge r)$

(3.42) **Contradiction**: $p \wedge \neg p \quad \equiv \quad \mathit{false}$